In the Claims:

Claims 1-8 (Cancelled).

9. (Previously Presented) A method for an entity different than a manufacturer of an integrated circuit card to perform a secure personalization phase of the semi-finished integrated circuit card, the integrated circuit card comprising a non-volatile memory storing an algorithm for processing data as a finite-state machine and enabling the entity different than the manufacturer of the integrated circuit card to access the algorithm for storing personalization data and information in the non-volatile memory required by the secure personalization phase according to a designated application field of the integrated circuit card, the method comprising:

performing a security authentication before enabling the algorithm to receive the personalization data and information;

enabling the algorithm to receive the personalization data and information;

storing the personalization data and information in secret memory locations in the non-volatile memory according to a data structure and an access procedure hidden to the entity different from the manufacturer of the integrated circuit card; and

repeating the enabling and storing if the personalization data and information were not correct.

10. (Previously Presented) A method according to Claim 9 further comprising storing in the non-volatile memory different personalization commands corresponding to different memory locations.

11. (Previously Presented) A method according to Claim 9 wherein the integrated circuit card comprises a microprocessor; and wherein the finite-state machine processes the personalization data and information according to an event triggered by a command sent to the microprocessor.

12. (Previously Presented) A method according to Claim 11 wherein transitions from one state to another state of the finite-state machine are activated by at least one of the following events: personalization process enabling, security authentication, data sending and personalization completion.

13. (Previously Presented) A method according to Claim 12 wherein each event is triggered by a set of commands sent to the integrated circuit card, the commands comprising at least one of enable personalization, verify personalization code, store personalization data and lock personalization.

14. (Previously Presented) A method according to Claim 13 wherein the enable personalization command allows transition on a ready state so that the integrated circuit card is enabled to receive the commands specified for the data personalization.

15. (Previously Presented) A method according to Claim 14 wherein the ready state is a transition state, and only the verify personalization code command is accepted.

16. (Previously Presented) A method for an entity different than a manufacturer of a smart card to perform a secure personalization phase of the semi-finished smart card, the smart card comprising a non-volatile memory storing an algorithm for processing data as a finite-state machine and enabling the entity different from the manufacturer of the smart card to access the algorithm for storing personalization data and information in the non-volatile memory required by the secure personalization phase, the method comprising:

performing a security authentication before enabling the algorithm to receive the personalization data and information;

enabling the algorithm to receive the personalization data;

storing the personalization data in secret memory locations in the non-volatile memory according to a data

structure and an access procedure hidden to the entity different from the manufacturer of the integrated circuit card; and

repeating the enabling and storing if the personalization data and information were not correct.

17. (Previously Presented) A method according to Claim 16 further comprising storing in the non-volatile memory different personalization commands corresponding to different memory locations.

18. (Previously Presented) A method according to Claim 16 wherein the smart card comprises a microprocessor; and wherein the finite-state machine processes the personalization data according to an event triggered by a command sent to the microprocessor.

19. (Previously Presented) A method according to Claim 18 wherein transitions from one state to another state of the finite-state machine are activated by at least one of the following events: personalization process enabling, security authentication, data sending and personalization completion.

20. (Previously Presented) A method according to Claim 19 wherein each event is triggered by a set of commands sent to the smart card, the commands comprising at least one of

enable personalization, verify personalization code, store personalization data and lock personalization.

21. (Previously Presented) A method according to Claim 20 wherein the enable personalization command allows transition on a ready state so that the smart card is enabled to receive the commands specified for the data personalization.

22. (Previously Presented) A method according to Claim 21 wherein the ready state is a transition state, and only the verify personalization code command is accepted.

23. (Previously Presented) An integrated circuit card comprising

a non-volatile memory for storing personalization data and information in secret allocations therein;

a microprocessor coupled to said non-volatile memory for performing a secure personalization phase of the integrated circuit card;

an algorithm stored in said non-volatile memory for processing data as a finite-state machine, the algorithm enabling an entity different from a manufacturer of the integrated circuit card to store the personalization data and information required by the secure personalization phase; and

said microprocessor for

performing security authentication before enabling said algorithm to receive the personalization data and information,

enabling said algorithm to receive the personalization data and information,

storing the personalization data and information in the secret allocations of said non-volatile memory according to a data structure and an access procedure hidden to the entity different from the integrated circuit card manufacturer, and

repeating the enabling and storing if the personalization data and information were not correct.

24. (Previously Presented) An integrated circuit card according to Claim 23 wherein said non-volatile memory stores different personalization commands corresponding to different memory locations.

25. (Previously Presented) An integrated circuit card according to Claim 23 wherein the finite-state machine processes the data according to an event triggered by a command sent to said microprocessor.

26. (Previously Presented) An integrated circuit card according to Claim 25 wherein transitions from one state to another state of the finite-state machine are activated by at

least one of the following events: personalization process enabling, security authentication, data sending and personalization completion.

27. (Previously Presented) An integrated circuit card according to Claim 26 wherein each event is triggered by a set of commands sent to said microprocessor, the commands comprising at least one of enable personalization, verify personalization code, store personalization data and lock personalization.

28. (Previously Presented) An integrated circuit card according to Claim 27 wherein the enable personalization command allows transition on a ready state so that said microprocessor is enabled to receive the commands specified for the data personalization.

29. (Previously Presented) An integrated circuit card according to Claim 28 wherein the ready state is a transition state, and only the verify personalization code command is accepted.

30. (Currently Amended) A method for manufacturing an integrated circuit card comprising a non-volatile memory, the method comprising:

storing an algorithm in the non-volatile memory for processing data as a finite-state machine; ~~and~~

defining a data structure and an access procedure hidden to an entity different from a manufacturer of the integrated circuit card for storing personalization data and information in the non-volatile memory required by a secure personalization phase according to a designated application field of the integrated circuit ~~card~~ card; and

storing in the non-volatile memory different personalization commands corresponding to different memory locations.

Claim 31 (Cancelled).

32. (Previously Presented) A method according to Claim 30 wherein the integrated circuit card comprises a microprocessor; and wherein the finite-state machine processes the personalization data and information according to an event triggered by a command sent to the microprocessor.

33. (Previously Presented) A method according to Claim 32 wherein transitions from one state to another state of the finite-state machine are activated by at least one of the following events: personalization process enabling, security authentication, data sending and personalization completion.

34. (Previously Presented) A method according to Claim 33 wherein each event is triggered by a set of commands

sent to the integrated circuit card, the commands comprising at least one of enable personalization, verify personalization code, store personalization data and lock personalization.

35. (Previously Presented) A method according to Claim 34 wherein the enable personalization command allows transition on a ready state so that the integrated circuit card is enabled to receive the commands specified for the data personalization.

36. (Previously Presented) A method according to Claim 35 wherein the ready state is a transition state, and only the verify personalization code command is accepted.